UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,438	12/05/2001	Neil Y. Iwamoto	36.P325	6310

5514 7590 11/20/2007	
FITZPATRICK CELLA HARPER & SCINTO	EXAMINER
30 ROCKEFELLER PLAZA	VU, THONG H
NEW YORK, NY 10112	

ART UNIT	PAPER NUMBER
2619	

MAIL DATE	DELIVERY MODE
11/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/017,438	IWAMOTO ET AL.
	Examiner	Art Unit	
	Thong H. Vu	2619	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-43* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

1.   Claims 17-43 are pending.

Continued Examination Under 37 CFR 1.114

2.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

10/19/07 has been entered.

Claim Objections

3.   Claim 17 is objected to because of the following informalities:

17. A method for controlling access to a peripheral device by a user, wherein the

peripheral device is accessible by the user based on access management information,

and wherein the peripheral device is constructed to provide the user with a plurality of

features and/or services including at least one of a printer service, a scanner service, a

facsimile service and a copy service, the method (comprising ?):

Appropriate correction is required.

Double Patenting

4.   The nonstatutory double patenting rejection is based on a judicially created doctrine
grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or
improper timewise extension of the "right to exclude" granted by a patent and to prevent possible
harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection
is appropriate where the conflicting claims are not identical, but at least one examined
application claim is not patentably distinct from the reference claim(s) because the examined
application claim is either anticipated by, or would have been obvious over, the reference
claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re
Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 17-43 are rejected on the ground of nonstatutory double patenting over claims 1-40 of U. S. Patent No. 5,647,056 ('056) since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows:

('056) 1. A method for managing access to a peripheral over a local area network with an interactive network board connectable to the peripheral via a bi-directional peripheral interface and connectable to the local area network via a local area network interface, the method comprising the steps of:

executing an access management program, which includes a socket server program, on the interactive network board, said socket server program including process steps to monitor a proprietary socket number for network communication to the proprietary socket, as well as process steps to issue commands to change operational and configuration status of the peripheral and to issue requests for current operational and configuration status of the peripheral;

monitoring, with said socket server program, the proprietary socket number to detect network communications directed by a client to the proprietary socket;

establishing direct communication via the proprietary socket between the socket server and the client so as to receive network communications;

commanding, with said socket server program via the bi-directional interface and in response to first ones of received network communications, the peripheral to change its operational and configuration status;

commanding, with said socket server program via the bi-directional interface and in response to second ones of received network communications, the peripheral to transmit its current operational and configuration status;

monitoring, with said socket server program, the bi-directional peripheral interface to detect and store current operational and configuration status transmitted from the peripheral; and

outputting, with said socket server program, the current operational and configuration status transmitted from the peripheral onto the local area network in response to the second ones of the received network communications.

32, A server for use in controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service and a copy service, the server comprising:

a reception unit constructed to receive, from a computer, authentication information corresponding to a user;

an **authentication unit** constructed to authenticate the user using the received authentication information; and

a transmission unit constructed to transmit, to the computer, access management information which specifies a feature and/or a service of the peripheral device available to the authenticated user from among the plurality of features and/or services of the peripheral device, or which specifies a feature and/or a service of the peripheral device not available to the authenticated user from among the plurality of features and/or services of the peripheral device,
wherein the computer transmits the access management information and a job to the peripheral device, the peripheral device determines, based on the transmitted access management information, whether the user can use the feature and/or a and/or the service of the peripheral device necessary to perform the job, and
the peripheral device performs the job in case that it is determined that the user can use the feature and/or the service necessary to perform the job.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See MPEP § 804.

Claim Rejections - 35 USC § 102

Claims 17-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Takaoka [7,006,259 B1].

5.   Claim 17, Takaoka discloses A method for controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is constructed to provide the user with a plurality of features and/or services including at least one of a printer service, a scanner service, a facsimile service and a copy service, the method (comprising):

receiving, at a computer, from a server [Takaoka, client-server, col 1 lines 55-60], access management information which specifies a feature and/or a service of the peripheral device available to the user from among the plurality of features and/or services of the peripheral device, or which specifies a feature and/or a service of the peripheral device not available to the user from among the plurality of features, and/or services of the peripheral device [Takaoka, managing information, col 5 lines 38-67];

receiving, at the peripheral device, the access management information and a job from the computer [Takaoka, received document, col 4 lines 1-20];

determining, at the peripheral device, whether the user can use the feature and/or the service of the peripheral device necessary to perform the received job, based on the

received access management information [Takaoka, guidance for subsequent operation

is displayed, col 6 lines 29-34]; and

performing, at the peripheral device, the received job in a case that it is <u>determined that</u>

the user can use the feature and/or the service necessary to perform the received job

[Takaoka, the user authentication is succeeded, and the subsequent transmission

operation can be performed, col 6 lines 55-60].

6.   Claim 18, Takaoka discloses receiving, at the server, authentication information

corresponding to the user from the computer; and authenticating, at the server, the user

based on the received authentication information, wherein the server transmits the

access management information to the computer after the server authenticates the user

[Takaoka, authentication, col 6 lines 55-60].

7.   Claim 19, Takaoka discloses the authentication information includes a username

and/or a password [Takaoka, password, F-code, col 1 line 23].

8.   Claim 20, Takaoka discloses transmitting, at the peripheral device, to the

computer, a message for denying the access by the user, in case that the peripheral

device receives the job without receiving the access management information for the

user as inherent feature of authentication.

9.   Claim 21, Takaoka discloses transmitting, at the peripheral device, to the

computer, a message for denying the job, in case that the user can not use the feature

and/or the service necessary to perform the received job as inherent feature of

authentication.

10.   Claim 22, Takaoka discloses transmitting, at the computer, to the server, a request for the access management information, wherein the request identifies the user and the peripheral device, wherein the computer receives the access management information corresponding to the user and the peripheral device as inherent feature of authentication.

11.   Claim 23, Takaoka discloses receiving, at the peripheral device, access management information for a second user from the server and not through the computer;

determining, at the peripheral device, a level of access to the peripheral device available to the second user based on the received access management information for the second user; and allowing, at the peripheral device, the second user access to the peripheral device based on the determined level of access to the peripheral device as a design choice.

12.   Claim 24, Takaoka discloses receiving, at the server, authentication information corresponding to the second user from the peripheral device; and authenticating, at the server, the second user based on the received authentication information, wherein the server transmits the access management information for the second user to the peripheral device after the server authenticates the second user as a design choice.

13.   Claim 37, Takaoka discloses at the peripheral device, the access management information is received along with the job from the computer as inherent feature of authentication.

14.   Claim 25, Takaoka discloses A method for controlling access to a peripheral

device by a user, wherein the peripheral device is accessible by the user based on

access management information, and wherein the peripheral device is constructed to

provide the user with a plurality of features and/or services including at least one of a

printer service, a scanner service, a facsimile service and a copy service, the method

comprising:

receiving, at a computer, from a server, access management information which

specifies a feature and/or a service of the peripheral device available to the user from

among the plurality of features and/or services of the peripheral device;

receiving, at the peripheral device, the access management information and a job from

the computer;

determining, at the peripheral device, whether the user can use-a-use the feature and/or

the service of the peripheral device necessary to perform the received job, based on the

received access management information [Takaoka, guidance for subsequent operation

is displayed, col 6 lines 29-34]; and

performing, at the peripheral device, the received job in a case that it is determined that

the user can use the feature and/or the service necessary to perform the received job

[Takaoka, the user authentication is succeeded, and the subsequent transmission

operation can be performed, col 6 lines 55-60].

15.   Claim 38, Takaoka discloses at the peripheral device, the access management

information is received along with the job from the computer [Takaoka, a network

control device, col 5 lines 25].

16.   Claim 26, Takaoka discloses A <u>peripheral</u> device which is accessible by a user

based on access management information, <u>and wherein the peripheral device is</u>

<u>constructed to provide the user with a plurality of features and/or services including at</u>

<u>least one of a printer service, a scanner service, a facsimile service and a copy service,</u>

comprising:

a reception unit constructed to receive, from a computer, a job and access management

information which specifies a feature and/or a service of the <u>peripheral</u> device available

to a user <u>from among the plurality of features and/or services of the peripheral device,</u>

<u>or which specifies</u> a feature and/or a service of the peripheral device not available to the

user <u>from among the plurality of features and/or services of the peripheral device,</u>

wherein the access management information is transmitted from a server to the

computer before the access management information is transmitted from the computer

to the <u>peripheral</u> device [Takaoka, a network control device, col 5 line 25]; and

a controller constructed to determine, based on the received access management

information, whether the user can use the feature a and/or <u>the</u> service of the <u>peripheral</u>

device necessary to perform the received job [Takaoka, guidance for subsequent

operation is displayed, col 6 lines 29-34], and constructed to perform the received job in

a case that <u>it is</u> determined that the user can use the feature and/or the service

necessary to perform the received job [Takaoka, the user authentication is succeeded,

and the subsequent transmission operation can be performed, col 6 lines 55-60].

17.   Claim 39, Takaoka discloses the reception unit receives, from the computer, the
access management information along with the job as a design choice.

18.   Claim 27, Takaoka discloses the <u>peripheral</u> device is <u>constructed to provide at</u>
<u>least the printer service</u> and the job is a print job as a design choice.

19.   Claim 28, Takaoka discloses a transmission unit constructed to transmit, to the
computer, a message for denying the access by the user, in case that said reception
unit receives the job without receiving the access management information for the user
[Takaoka, authentication, col 6 lines 55-60].

20.   Claim 29, Takaoka discloses a transmission unit constructed to transmit, to the
computer, a message for denying the job, in case that the user can not use the feature
and/or the service necessary to perform the received job [Takaoka, authentication, col 6
lines 55-60].

21.   Claim 30, Takaoka discloses said reception unit receives access management
information for a second user from the server without <u>and not through</u> the computer,
said controller determines a level of access to the device available to the second user
based on the received access management information for the second user, and
said controller allows the second user access to the device based on the
determined level of access to the device as a design choice.

22.   Claim 31, Takaoka discloses A <u>peripheral</u> device which is accessible by a user
based on access management information, <u>and wherein the peripheral device is</u>

constructed to provide the user with a plurality of features and/or services including at

least one of a printer service, a scanner service, a facsimile service and a copy service,

comprising:

a reception unit constructed to receive, from a computer, a job and access management

information which specifies a feature and/or a service of the peripheral device available

to the user from among the plurality of features and/or services of the peripheral device,

wherein the access management information is transmitted from a server to the

computer before the access management information is transmitted from the computer

to the peripheral device [Takaoka, a network control device, col 5 line 25]; and

a controller constructed to determine, based on the received access management

information, whether the user can use the feature and/or the service of the peripheral

device necessary to perform the received job [Takaoka, guidance for subsequent

operation is displayed, col 6 lines 29-34], and constructed to perform the received job in

case that it is determined that the user can use the feature and/or the service necessary

to perform the received job [Takaoka, the user authentication is succeeded, and the

subsequent transmission operation can be performed, col 6 lines 55-60].

23.   Claim 40, Takaoka discloses the reception unit receives, from the computer, the

access management information along with the job as a design choice.

24.   Claim 32, Takaoka discloses A server for use in controlling access to a

peripheral device by a user, wherein the peripheral device is accessible by the user

based on access management information, and wherein the peripheral device is

constructed to provide the user with a plurality of features and/or services including at

least one of a printer service, a scanner service, a facsimile service and a copy service,

the server comprising:

a reception unit constructed to receive, from a computer, authentication information

corresponding to a user [Takaoka, received document, col 6 line 1-20];

an authentication unit constructed to authenticate the user using the received

authentication information; and a transmission unit constructed to transmit, to the

computer, access management information which specifies a feature and/or a service of

the peripheral device available to the authenticated user from among the plurality of

features and/or services of the peripheral device, or which specifies a feature and/or a

service of the peripheral device not available to the authenticated user from among the

plurality of features and/or services of the peripheral device, [Takaoka, authentication,

col 6 lines 55-60]

wherein the computer transmits the access management information and a job to

the peripheral device [Takaoka, a network control device, col 5 line 25],

the peripheral device determines, based on the transmitted access management

information, whether the user can use the feature and/or the service of the peripheral

device necessary to perform the job [Takaoka, guidance for subsequent operation is

displayed, col 6 lines 29-34], and

the peripheral device performs the job in case that it is determined that the user can use

the feature and/or the service necessary to perform the job [Takaoka, the user

authentication is succeeded, and the subsequent transmission operation can be performed, col 6 lines 55-60].

25.   Claim 41, Takaoka discloses the computer transmits the access management information along with the job to the peripheral device as a design choice.

26.   Claim 33, Takaoka discloses said reception unit receives, from the peripheral device, authentication information corresponding to a second user, said authentication unit authenticates the second user using the received authentication information corresponding to the second user, said transmission unit transmits, to the peripheral device, access management information which specifies a feature and/or a service of the peripheral device available to the second user from among the plurality of features and/or services of the peripheral device, or which specifies a feature and/or a service Of the peripheral device not available to the second user from among the plurality of features and/or services of the peripheral device, the peripheral device determines a level of access to the peripheral device available to the second user based on the access management information for the second user, and the peripheral device allows the second user access to the peripheral device based on the determined level of access to the peripheral device as a design choice.

27.   Claim 34, Takaoka discloses A server for use in controlling access to a peripheral, device by a user, wherein the peripheral device is accessible by the user based on access management information, and wherein the peripheral device is

constructed to provide the user with a plurality of features and/or services including at

least one of a printer service, a scanner service, a facsimile service and a copy service,

the server comprising:

a reception unit constructed to receive, from a computer, authentication information

corresponding to a user [Takaoka, received document, col 6 line 8];

an authentication unit constructed to authenticate the user using the received

authentication information [Takaoka, authentication, col 6 lines 55-60]; and

a transmission unit constructed to transmit, to the computer, access management

information which specifies a feature and/or a service of the peripheral device available

to the authenticated user from among the plurality of features and/or services of the

peripheral device [Takaoka, document managing information, col 5 lines 38-67]

wherein the computer transmits the access management information and a job to the

peripheral device [Takaoka, a network control device, col 5 line 25],

the peripheral device determines, based on the transmitted access management

information, whether the user can use the feature and/or the service of the peripheral

device necessary to perform the job [Takaoka, guidance for subsequent operation is

displayed, col 6 lines 29-34], and

the peripheral device performs the job in case that it is determined that the user can use

the feature and/or the service necessary to perform the job [Takaoka, the user

authentication is succeeded, and the subsequent transmission operation can be

performed, col 6 lines 55-60].

28.   Claim 42, Takaoka discloses the computer transmits the access management

information along with the job to the peripheral device as a design choice.

29.   Claim 35, Takaoka discloses A computer for transmitting a job to a peripheral

device, wherein the peripheral device is accessible by a user based on access

management information, and wherein the peripheral device is constructed to provide

the user with a plurality of features and/or services including at least one of a printer

service, a scanner service, a facsimile service and a copy service, the computer

comprising:

a reception unit constructed to receive, from a server, access management information

which specifies a feature and/or a service of the peripheral device available to a user

from among the plurality of features and/or services of the peripheral device, or which

specifies a feature and/or a service of the peripheral device not available to the user

from among the plurality of features and/or services of the peripheral device [Takaoka,

authentication, col 6 lines 55-60]; and

a transmission unit constructed to transmit the received access management

information and a job to the peripheral device [Takaoka, a network control device, col 5

line 25]

wherein the peripheral device determines whether the user can use the feature and/or

the service of the peripheral device necessary to perform the job, based on the

transmitted access management information [Takaoka, guidance for subsequent

operation is displayed, col 6 lines 29-34], and

the peripheral device performs the job in case that <u>it is determined that</u> the user can use

the feature and/or the service necessary to perform the job [Takaoka, the user

authentication is succeeded, and the subsequent transmission operation can be

performed, col 6 lines 55-60].

30.   Claim 36, Takaoka discloses a second transmission unit constructed to transmit,

to the server, authentication information corresponding to the user, wherein the server

authenticates the user using the authentication information and transmits the access

management information for the authenticated user to the computer [Takaoka,

authentication, col 6 lines 55-60].

31.   Claim 43, Takaoka discloses the transmission unit transmits the received access

management information along with the job to the peripheral device as a design choice.

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Thong H. Vu whose telephone number is 571-272-3904. The
examiner can normally be reached on 6:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, *Jay Patel* can be reached on 571-272-2988. The fax phone number for the
organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent
Application Information Retrieval (PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR
system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
like assistance from a USPTO Customer Service Representative or access to the automated
information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thong Vu
Primary Examiner

THONG VU
PRIMARY PATENT EXAMINER